

Exfiltrácia citlivých dát cez neidentifikovaný USB

Vyšetrovatel': Vadym Shevchuk

Link na prezentáciu: <https://bcstudent.fpvucm.sk/~shevchukvadym/dfa/prezentacia.pdf>

Opis prípadu:

Spoločnosť SecureSoft zaznamenala únik dôverných dokumentov týkajúcich sa pripravovaných bezpečnostných algoritmov, ktoré sa objavili na verejnom fóre. Prístup k týmto súborom mali len vybraní zamestnanci. Interné vyšetrovanie odhalilo, že v čase incidentu bolo k vývojárskemu počítaču pripojené neznáme USB zariadenie. Zároveň bol v serverovni nájdený USB kľúč, ktorý nepatril žiadnemu zamestnancovi. Existuje podozrenie, že kľúč bol použitý na exfiltráciu údajov alebo obsahoval škodlivý softvér.

5WH

Who? – Kto?

Osoba s prístupom k vývojárskemu počítaču alebo so vstupom do serverovne. Môže ísť o interného zamestnanca alebo osobu, ktorá získala fyzický prístup k systému bez autorizácie.

What? – Čo?

Došlo k úniku citlivých dokumentov týkajúcich sa bezpečnostných algoritmov. Súbor sa objavil na verejnom fóre a existuje podozrenie, že boli prenesené pomocou neznámeho USB zariadenia.

When? – Kedy?

Incident pravdepodobne nastal v časovom intervale zistenom zo systémových logov, keď bolo USB zariadenie pripojené k vývojárskemu počítaču. Presný čas bude stanovený forenznou analýzou.

Where? – Kde?

V serverovni spoločnosti SecureSoft, kde bolo USB zariadenie fyzicky nájdené.

Why? – Prečo?

Motívom mohol byť zámer získať dôverné informácie na vlastné využitie, ich predaj konkurencii alebo iný neoprávnený účel. Alternatívne mohlo ísť o nevedomé konanie s bezpečnostnými následkami.

How? – Ako?

Únik údajov mohol nastať manuálnym kopírovaním súborov na USB kľúč alebo automaticky prostredníctvom škodlivého skriptu spusteného po jeho pripojení k systému.

Očakávaný výsledok

- Určenie, či boli citlivé dáta skopírované na USB kľúč.
- Zistenie, či USB obsahovalo škodlivý softvér na automatické získanie údajov.

Hypotéza 1: Úmyselné kopírovanie dôverných dokumentov

Neautorizované USB zariadenie bolo použité na manuálny prenos citlivých súborov z vývojárskeho počítača osobou s oprávneným prístupom.

Ako hypotézu overíme:

- Vytvoríme forenznú kópiu USB zariadenia (napr. pomocou FTK Imager).
- Pomocou nástrojov ako Autopsy porovnáme hash súborov na USB s internými dokumentmi.
- Hypotéza bude potvrdená, ak nájdeme zhodné dokumenty a vieme ich časovo a používateľsky priradiť ku konkrétnej aktivite.

Hypotéza 2: Automatizovaná exfiltrácia údajov cez škodlivý skript

USB kľúč obsahoval skript, ktorý po pripojení automaticky spustil proces získavania dát bez vedomia používateľa.

Ako hypotézu overíme:

- Analyzujeme obsah USB na prítomnosť skriptov (napr. autorun.inf, PowerShell, Bash).
- Hypotéza bude potvrdená, ak sa nájde aktívny alebo zvyškový kód, ktorý sa spustil automaticky a vykonával nežiaduce operácie.

Hypotéza 3: USB kľúč nebol použitý na únik dôverných dokumentov

Predpokladá sa, že neznáme USB zariadenie neobsahuje žiadne citlivé interné súbory spoločnosti a neslúžilo ako médium na exfiltráciu dokumentov týkajúcich sa pripravovaných bezpečnostných algoritmov.

Ako hypotézu overíme:

- Vytvoríme forenznú kópiu USB zariadenia a vykonáme analýzu všetkých dostupných aj obnovených súborov.
- Porovnáme hashe súborov na USB s hashmi dôverných firemných dokumentov.
- Skontrolujeme, či sa na zariadení nenachádzajú fragmenty alebo stopy po citlivých súboroch.
- Hypotéza bude potvrdená, ak sa žiadne zhodné alebo súvisiace dokumenty na USB zariadení nenájdu.

Príprava dát

Pre analýzu bude využitý dataset <http://roussev.net/t5/t5.html>, ktorý obsahuje 4 457 súborov (.html, .pdf, .doc, .ppt, .jpg, .xls, .gif). Okrem toho boli pridané aj Windows logy a škodlivé skripty. Počas analýzy sa budú vyhľadávať škodlivé skripty a dôverné PDF dokumenty, ktoré mohli byť predmetom neoprávneného prenosu. Veľkosť: 2.98Gb.

Zariadenia prítomné na mieste incidentu

- **Vývojársky počítač** – stanica člena tímu s prístupom k citlivým údajom. V čase incidentu k nemu bolo pripojené neautorizované USB zariadenie, ktoré mohlo slúžiť na kopírovanie dokumentov.
- **Neznáme USB zariadenie** – nájdené v serverovni, bez evidencie vlastníctva. Môže obsahovať skopírované dáta alebo škodlivý kód. Je predmetom forenznej analýzy.

Nájdenný USB kľúč



Parametre zariadenia:

Kapacita úložiska (celková): 128 GB

Rozhraní: USB 3.2 Gen 1 (USB 3.0)

Konektor: USB-A

Rýchlosť čítania: 100 MB/s

Rýchlosť zápisu: 10 MB/s

Materiál: Plast

Farba: Červená, Čierna

Šírka: 67,4 mm

Výška: 11,6 mm

Dĺžka: 21,8 mm

Hmotnosť: 10 g

Analýza RAM pamäte

Po analýze obrazu RAM pamäte bolo potvrdené, že dany USB kľúč bol pripojený k vývojáorskému počítaču a mohol byť použitý na exfiltráciu údajov alebo obsahoval škodlivý softvér.

00F787070	00 67 00 65 00 2D 00 43 00 6C 00 61 00 73 00 73	.g.e.-.C.l.a.s.s
00F787080	00 50 00 6E 00 50 00 2F 00 4F 00 70 00 65 00 72	.P.n.P./O.p.e.r
00F787090	00 61 00 74 00 69 00 6F 00 6E 00 61 00 6C 00 0C	.a.t.i.o.n.a.l..
00F7870A0	01 58 A9 B5 43 0F 08 00 00 0F 00 00 00 10 00 0F	.X@uC.....
00F7870B0	00 04 00 08 00 09 00 02 00 11 00 02 00 05 00 02	
00F7870C0	00 0D 00 02 00 04 00 14 00 01 00 04 00 01 00 04	
00F7870D0	00 01 00 04 00 01 00 04 00 01 00 04 00 04 00 08	
00F7870E0	00 06 00 0E 00 01 00 04 00 0A 1C 0F CE 34 89 E8	Î4kè
00F7870F0	A5 D3 5F FC 02 5D B4 9B 05 02 00 00 00 4B 69 6E	ŸÓ ü.]´>.....Kin
00F787100	67 73 74 6F 6E 00 44 61 74 61 54 72 61 76 65 6C	gston.DataTravel
00F787110	65 72 20 33 2E 30 00 50 4D 41 50 00 36 42 30 46	er 3.0.PMAP.6B0F
00F787120	41 37 34 31 34 31 43 39 00 85 01 00 C0 84 02 05	A74141C9.....À„...
00F787130	24 00 06 00 00 00 1E 00 00 00 01 00 00 00 00 00	\$.....
00F787140	00 00 00 00 00 02 00 00 2A 2A 00 00 00 02 00 00	**.....
00F787150	4A 00 00 00 00 00 00 00 07 24 CA 47 D2 6F DA 01	J.....\$ÊGÒoÚ.
00F787160	0F 01 01 00 0C 01 1D 21 C2 C5 EE 1F 00 00 12 00	!ÂÂî.....

Informácie z FTK Imager

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 01

Evidence Number: 001

Unique description: USB

Examiner: User

Notes: Kingstone 128

Information for D:\ramimage\obrazUSB:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 15,042

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 241,660,916

[Physical Drive Information]

Drive Model: Kingston DataTraveler 3.0 USB Device

Drive Serial Number: 20

Drive Interface Type: USB

Removable drive: True

Source data size: 117998 MB

Sector count: 241660916

[Computed Hashes]

MD5 checksum: d10335337a68293e8d5e42bcacd1a596

SHA1 checksum: a2580c3f85d2a782decf320f7a2a5d4512adc9d4

Image Information:

Acquisition started: Sat Mar 22 10:26:22 2025

Acquisition finished: Sat Mar 22 10:38:34 2025

Segment list:

D:\ramimage\obrazUSB.001

COMPUTED HASH : d10335337a68293e8d5e42bcacd1a596

COMPUTED HASH : a2580c3f85d2a782decf320f7a2a5d4512adc9d4

Image Verification Results:

Verification started: Sat Mar 22 10:38:34 2025

Verification finished: Sat Mar 22 10:44:20 2025

MD5 checksum: d10335337a68293e8d5e42bcacd1a596 : verified

SHA1 checksum: a2580c3f85d2a782decf320f7a2a5d4512adc9d4 : verified

Výsledky overenia obrazu

[-]	
Name	obrazUSB.001
Sector count	241660916
[-] MD5 Hash	
Computed hash	d10335337a68293e8d5e42bcacd1a596
Report Hash	d10335337a68293e8d5e42bcacd1a596
Verify result	Match
[-] SHA1 Hash	
Computed hash	a2580c3f85d2a782decf320f7a2a5d4512adc9d4
Report Hash	a2580c3f85d2a782decf320f7a2a5d4512adc9d4
Verify result	Match
[-] Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Použité nástroje:

- **FTK Imager** – vytvorenie forenzného obrazu
- **Autopsy** – analýza image súboru (kategorizácia, vyhľadávanie)
- **HxD** – hexadecimálna analýza

Bezpečnostné opatrenia

1. Fyzická ochrana.

- Počas prepravy bol kľúč prepravovaný v bezpečnostnom puzdre s evidenciou odovzdania a prevzatia.
- Prístup k zariadeniu mali výhradne autorizované osoby.

2. Digitálna ochrana

- Pri analýze sa použil write-blocker, aby sa predišlo akýmkoľvek zmenám dát na zariadení.
- Forenzný obraz USB bol vytvorený čo najskôr po jeho zaistení pomocou nástroja FTK Imager

3. Izolované prostredie

- Analýza dát bola vykonaná v offline prostredí – počítač nebol pripojený k žiadnej sieti

4. Dokumentácia a evidencia

- Všetky manipulácie so zariadením boli zaznamenávané do reťazca starostlivosti (Chain of Custody).

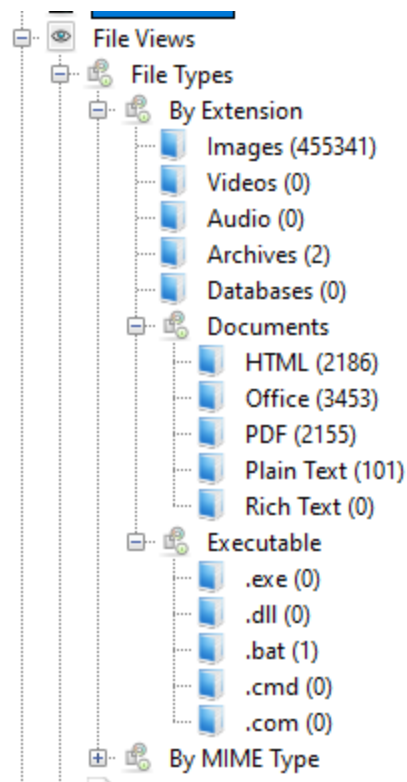
Bitové kópie:

- **Pracovná kópia:** uložená na notebooku forenzného analytika (Lenovo ThinkPad, disk C:\Forensics\Cases\USB-incident.E01)
- **Archivná kópia:** uložená na externom, zašifrovanom HDD (uložený v zamknutom trezore spoločnosti SecureSoft)

Kategórie súborov určené na analýzu + počet súborov

- **PDF dokumenty** – 2155 súborov
Obsahujú technické špecifikácie bezpečnostných algoritmov, ktoré sa objavili na verejnom fóre. Budú analyzované ich názvy, obsah, hash hodnoty a časové pečiatky.
- **Skripty a konfiguračné súbory** (napr. .bat, .ps1, autorun.inf) – 1 súbor
Potenciálne automatizačné skripty, ktoré mohli byť použité na exfiltráciu dát bez zásahu používateľa.

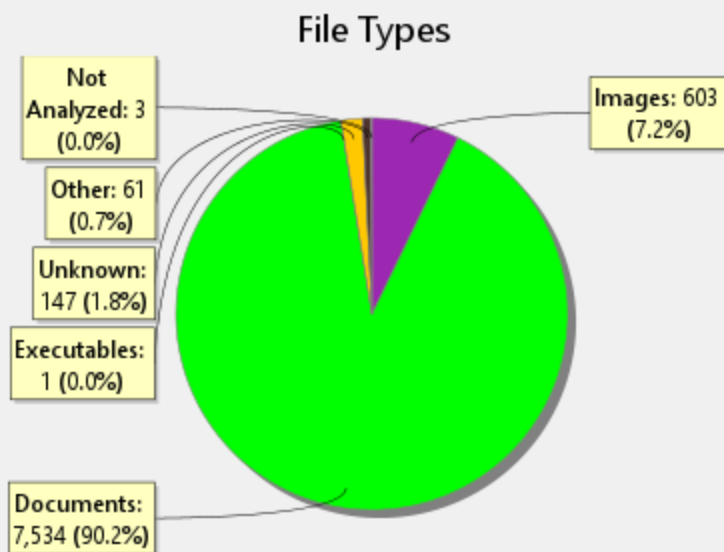
Kategórie údajov



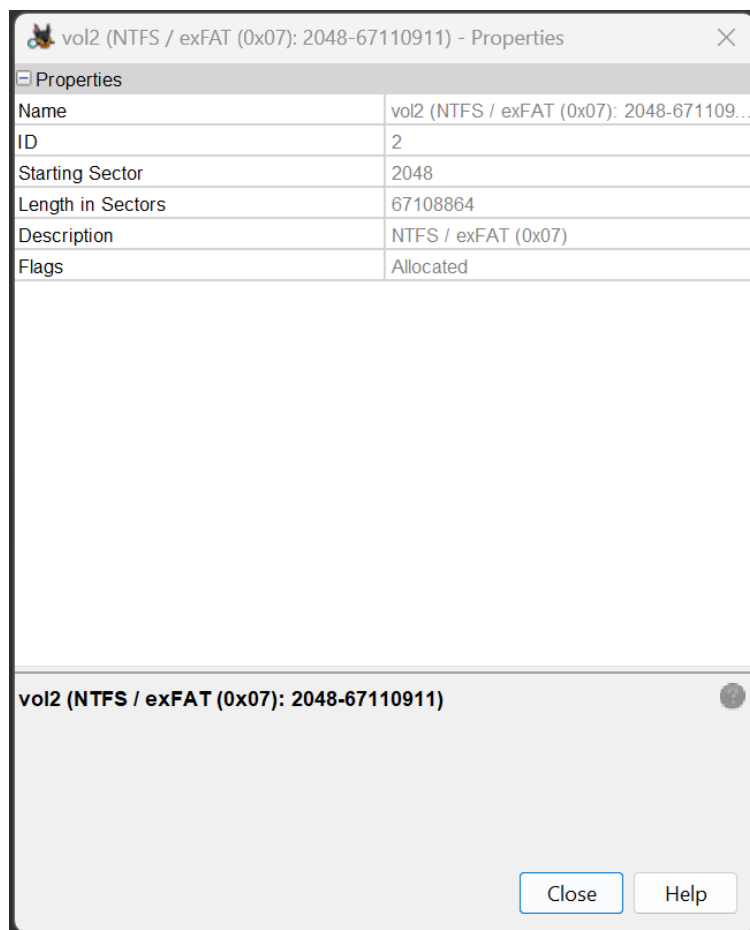
Usage:

OS:

Size: 124 GB



Umiestnenie súborov a použitý súborový systém



Na základe opisu (0x07) a systémovej analýzy možno potvrdiť, že **použitý súborový systém je buď NTFS alebo exFAT**, čo sú bežné formáty pre USB úložiská s vyššou kapacitou.

Umiestnenie súborov je v rámci analyzovaného zväzku vol2, ktorý začína na sektore **2048**.

Potreba metadát, EXIF údajov, logov, temp súborov, SQL dát, IP adries:

- **Metadáta:** Nie sú potrebné
Zameriavame sa na konkrétne súbory (napr. PDF) a ich obsah, nie na časové pečiatky. Prioritou je overenie výskytu uniknutých dát, nie presný čas manipulácie.
- **EXIF údaje:** Nie sú potrebné
Analýza sa netýka obrázkov ani fotiek. Na USB kľúči neboli nájdené žiadne relevantné multimediálne súbory.
- **Logy:** Áno, budú potrebné
Dôležité pre identifikáciu pripojenia USB k vývojárskemu počítaču.
- **Temp súbory:** Áno, budú potrebné
Môžu obsahovať zvyškové dáta alebo potvrdenie o práci so súbormi.

- **SQL dáta:** Nie sú potrebné
V prípade neboli identifikované žiadne aplikácie využívajúce interné databázy. Nie je predpoklad práce s .sqlite alebo .db súbormi.
- **IP adresy:** Nie sú potrebné
V prípade neboli zachytené sieťové dáta (napr. .pcap), exfiltrácia prebehla lokálne cez fyzické pripojenie USB.

Chain of Custody

Číslo:	001	Typ súboru:	raw	Obnovený súbor:	Nie	Veľkosť:	15.9 GB
Popis prípadu:		USB kľúč z serverovne analyzovaný pre podozrenie z úniku dát.					
Názov súboru:		Unik.raw					
Miesto získania digitálnej stopy:		Serverovňa spoločnosti SecureSoft					
Poznámky:							
Časové pečiatky							
Access:	12.04.2025, 17:32		Modify:	12.04.2025, 18:12		Change:	12.04.2025, 21:37
Digitálna odtlačok (heš)	MD5	3a5d9c5b3df764e2d89b71df9a8e2b1a					
	SHA1	d6c73bdfb7e34998e6ef9cb0c05e2d85987d77a2fd2341cdabdbfd2e15a30c94					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
12.04.2025, 18:12		Začiatok analýzy obsahu USB v nástroji Autopsy vo forenznom prostredí					
12.04.2025, 21:37		Ukončenie analýzy, záloha výstupov a vypracovanie forenznej správy					

Vyhodnotenie hypotéz

Hypotéza 1: Úmyselné kopírovanie dôverných dokumentov

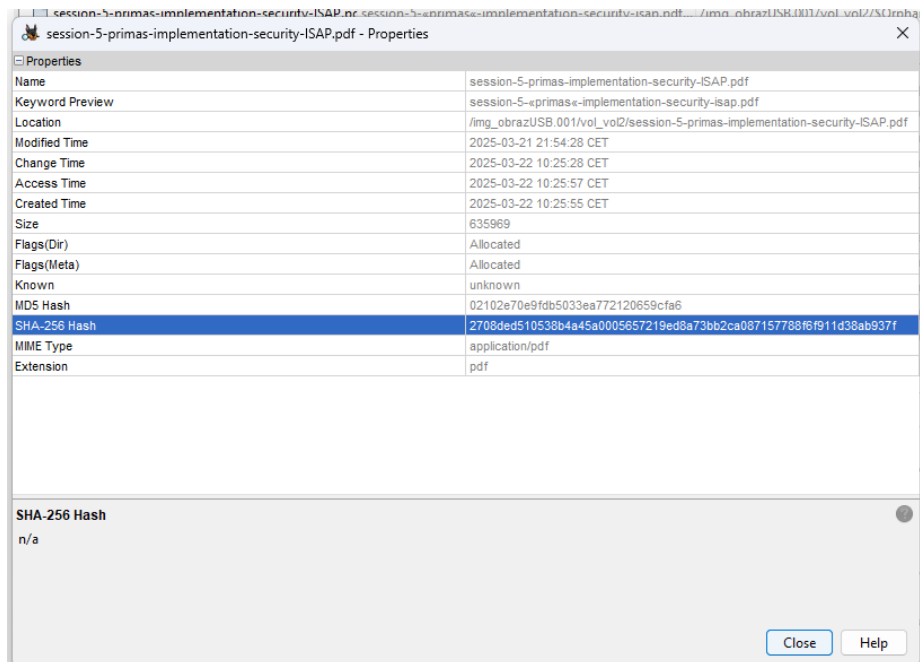
Stav: Potvrdená

Spôsob overenia:

Na analyzovanom USB zariadení boli nájdené dva dôverné dokumenty:

- biocts_2014_iso_iec_user_guide.pdf
- session-5-primas-implementation-security-ISAP.pdf

Pomocou nástroja na výpočet hash hodnôt boli **porovnané ich SHA-256 hashe** s originálnymi súbormi uloženými na internom serveri. Výsledky boli **zhodné**, čo potvrdzuje, že súbory boli **identicky skopírované** na neautorizované zariadenie.



SHA256 File Checksum

This SHA256 online tool helps you calculate the hash of a file from local or URL using SHA256 without uploading the file. It also supports HMAC.

Settings

Hash

Auto Update

Remember Input

Input Type

File

Output Encoding

Hex (Lower Case)

Enable HMAC

Input

session-5-primas-implementation-security-ISAP.pdf

Output

2708ded510538b4a45a0005657219ed8a73bb2ca087157788f6f911d38ab937f

SHA256 File Checksum

This SHA256 online tool helps you calculate the hash of a file from local or URL using SHA256 without uploading the file. It also supports HMAC.

settings

Hash

Auto Update

Remember Input

Input Type

File

Output Encoding

Hex (Lower Case)

Enable HMAC

Input

biocets_2014_iso_iec_user_guide.pdf

biocets_2014_iso_iec_user_guide.pdf

Output

b23e3f26fcd3368ea08383a0d34c27443a0b23ac7fedf8488b491925b697c04

Properties	
Name	biocets_2014_iso_iec_user_guide.pdf
Keyword Preview	er_guide.pdf «BioCTS» for ISO/IEC Binary and
Location	/img_obrazUSB.001/vol_vol2/biocets_2014_iso_iec_user_guide.pdf
Modified Time	2025-03-21 21:53:42 CET
Change Time	2025-03-22 10:25:24 CET
Access Time	2025-03-22 10:25:53 CET
Created Time	2025-03-22 10:25:38 CET
Size	1573445
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
MD5 Hash	a3c7fe84f20e370b4294c8c0ce110ecf
SHA-256 Hash	b23e3f26fcd3368ea08383a0d34c27443a0b23ac7fedf8488b491925b697c04
MIME Type	application/pdf
Extension	pdf

Properties

Properties of this object.

Close

Help

Hypotéza 2: Automatizovaná exfiltrácia údajov cez škodlivý script

Stav: Potvrdená

Spôsob overenia:

Na USB zariadení bol nájdený skript s názvom copy_documents.bat, ktorý obsahoval príkazy na automatické kopírovanie súborov z konkrétnych adresárov (napr.

C:\Users\DevTeam\Documents) do koreňového adresára USB.

Skript bol nastavený tak, aby sa spustil ihneď po pripojení zariadenia k systému, čím podporuje podozrenie, že exfiltrácia dát mohla prebehnúť **automaticky, bez zásahu používateľa**.

Záver

Forenzná analýza potvrdila, že neidentifikované USB zariadenie bolo použité na úmyselnú exfiltráciu dôverných dokumentov zo systému spoločnosti SecureSoft. Na zariadení sa nachádzali dve citlivé PDF súbory s hashmi zhodnými s originálmi a škodlivý skript `copy_documents.bat`, ktorý umožňoval automatické kopírovanie súborov. Tieto zistenia vylučujú možnosť náhodného alebo neškodného použitia USB a potvrdzujú, že išlo o cieľený bezpečnostný incident. Všetky kroky vyšetrovania boli zdokumentované v súlade s princípmi reťazca starostlivosti o dôkaz.